HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/656,634	09/07/2000	Babak Tehranchi	81399N-R	1654

1333 7590 03/31/2006

BETH READ
PATENT LEGAL STAFF
EASTMAN KODAK COMPANY
343 STATE STREET
ROCHESTER, NY 14650-2201

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/656,634
Filing Date: September 07, 2000
Appellant(s): TEHRANCHI, BABAK

Nelson A. Blish
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 20 January 2006 appealing from the Office action mailed 29 August 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,963,909	WARREN	10-1999
6,735,311	RUMP	05-2004
5,774,546	HANDELMAN	6-1998
6,137,763	DAHAN	10-2000

5,959,717	CHAUM	9-1999
6,141,530	RABOWSKY	10-2000

Schneier, Bruce. Applied Cryptography, second edition, 1996, pp. 372-373.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claim 3 recites the limitation "said single data block" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

4. Claims 62-71 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are for a data structure alone, which is non-statutory subject matter because it is not embodied within a computer readable medium (MPEP 2106).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 28, 30, 32-36, 38-41, 43, 44, 52, 58, 62-69, 73 are rejected under 35 U.S.C. 102(e) as being anticipated by Warren, U.S. Patent No. 5,963,909. Referring to claims 1, 28, 30, 32, 34, 58, Warren discloses a copy management system for multi-media wherein multi-media data is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56), which meets the limitation of partitioning the digital motion image data stream into a plurality of digital motion image data blocks, an encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks. Figure 12 shows explicitly that each data block contains the encryption key for the frame contained in the next data block, which meets the limitation of block synchronization index indicating a correspondence between said encryption key and single data block. Figure 12 shows a multi-media data stream that has been encrypted with the corresponding keys (Col. 13, line 58 – Col. 14, line 3), which meets the limitation of an encryption engine that, for each said single data block, produces an encrypted data block using said encryption key fro said encryption key generator. The multi-media data stream is transmitted over a data channel (Col. 2, lines 27-34), which meets the limitation of a data transmission channel for delivering said encryption data block from said encryption engine to the digital data receiver. The multi-media data stream could include a plurality of data channels, with one of the data channels including the encryption key data (Col. 2, lines 27-34), which meets the limitation of a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver. As specified above, the encryption key data also provides the means for the block synchronization as disclosed in Figure 12, which meets the limitation of a block synchronization data channel for delivering said block

synchronization index from said encryption key generator to the digital data receiver. Warren reference does not disclose that the synchronization index is used to map each key in a memory to a respective encrypted data block is not persuasive because the data block synchronizes the keys to corresponding sequential frames (Figure 12), and the key stream is sent to the decryption unit for decryption of the data stream. Since the key stream is ordered from the data block, the decryption unit would receive the key stream in the same order. Therefore, when the decryption unit stores the key stream to perform the decryption operation, the keys would be mapped in the memory to a respective encrypted data block.

Referring to claims 40, 41, Warren discloses that the multi-media data is video (Abstract).

Referring to claims 33, 35, Warren discloses that the encrypted data is recorded on a medium (Fig. 15, 140).

Referring to claim 36, Warren discloses a copy management system for multi-media wherein multi-media data is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56). The multi-media data stream could include a plurality of data channels, with one of the data channels including the encryption key data (Col. 2, lines 27-34), which meets the limitation of providing said plurality of encryption keys separately from said encrypted data blocks. Figure 12 shows explicitly that each data block contains the encryption key for the frame contained in the next data block, which meets the limitation providing an identifier that correlates a mapping algorithm to said plurality of encryption keys.

Referring to claim 38, Warren discloses that NULL keys can be used to created unencrypted data blocks (Col. 14, lines 18-21), which meets the limitation of padding said plurality of encryption keys using dummy bits.

Referring to claim 39, Warren discloses that the receiver contains a decryption engine (Fig. 17) to decrypt the encrypted multi-media stream with the encryption keys that are embedded in the stream (Fig. 12, Col. 13, line 58 – Col. 14, line 3), which meets the limitation of digital receiver includes a decryption engine which is responsive to said encryption key and said encryption engine and decryption engine are provided with symmetric encryption, the encrypted data blocks comprise digital motion image data blocks and the digital motion image data blocks are decrypted by providing a digital motion image data frame or digital motion image data frame component identification; and generating a corresponding key from the plurality of encryption keys for use in decrypting the block of which the frame or frame component forms a part.

Referring to claim 43, Warren discloses that the data can be compressed (Col. 2, lines 31-33), which meets the limitation of single data block is compressed.

Referring to claim 44, Warren discloses that the compression can be done using MPEG compression methods (Col. 5, line 4).

Referring to claims 62, 64, Warren discloses in Figure 12 that the data stream as a field that identifies each frame, which are encrypted, and a field for the encryption key of each specific frame. This meets the limitations of a component ID field having plural bits mapping informaiton for identifying an image frame of the image block at which a specific encryption key is first used, an encryption key field of plural bits forming the encryption key and being operative for use in decrypting the image block.

Referring to claims 63, 65, Warren discloses in Figure 12 that the stream identifies the start of the data structure.

Referring to claim 66, Warren discloses in Figure 12 that the data stream as a field that identifies each frame. Figure 12 shows explicitly that each data block contains the encryption key for the frame contained in the next data block, which meets the limitation a synchronization field containing synchronization index information operative to link individual keys to respective blocks of video image data, each block comprising plural frames of the motion picture, a key field representing plural encryption keys that are operative for use in the decryption of respective image blocks.

Referring to claims 67, 68, Warren discloses in Figure 12 that keys and the frames are in sequential order, which meets the limitation of a key overhead field having informaiton indicating how keys are arranged in the key field and having information indicating how the blocks of video images data are structured.

Referring to claim 69, Warren discloses that the encryption key for a given frame is located in the next frame (Figure 12), which meets the limitation of a key overhead field having informaiton specifying an algorithm used to locate a corresponding key within the key field.

Referring to claim 73, Warren discloses in Figure 12 that the data stream as a field that identifies each frame, which are encrypted, and a field for the encryption key of each specific frame. Figure 17 shows the encrypted data stream being decrypted using the encryption keys taken from each encrypted frame, which meets the limitation of providing an identification of an image frame to be decrypted, providing a synchronization index to map a plurality of encryption keys, the keys being suited for use in decrypting respective blocks of image data forming a motion picture, in response to the identification of the image frame and the synchronization index outputting a corresponding key for decrypting of the specific image frame.

Referring to claim 77, Warren discloses in Figure 12 that each frame has a corresponding encryption key.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. Claims 1-3, 5-10, 13, 15, 16, 20-25, 27, 29, 47, 57, 58, 72, 74, 75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Rump, U.S. Patent No. 6,735,311. Referring to claims 1, 3, 20, 29, 47, 57, 58, 72, 74, 75, Warren discloses a copy management system for multi-media wherein multi-media data is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56), which meets the limitation of an encryption key generator for providing an encryption key assigned to each single

data block of the plurality of data blocks. Figure 12 shows explicitly that each data block contains the encryption key for the frame contained in the next data block, which meets the limitation of block synchronization index indicating a correspondence between said encryption key and single data block. Figure 12 shows a multi-media data stream that has been encrypted with the corresponding keys (Col. 13, line 58 – Col. 14, line 3), which meets the limitation of an encryption engine that, for each said single data block, produces an encrypted data block using said encryption key fro said encryption key generator. The multi-media data stream is transmitted over a data channel (Col. 2, lines 27-34), which meets the limitation of a data transmission channel for delivering said encryption data block from said encryption engine to the digital data receiver. The multi-media data stream could include a plurality of data channels, with one of the data channels including the encryption key data (Col. 2, lines 27-34), which meets the limitation of a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver. As specified above, the encryption key data also provides the means for the block synchronization as disclosed in Figure 12, which meets the limitation of a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver. Warren reference does not disclose that the synchronization index is used to map each key in a memory to a respective encrypted data block is not persuasive because the data block synchronizes the keys to corresponding sequential frames (Figure 12), and the key stream is sent to the decryption unit for decryption of the data stream. Since the key stream is ordered from the data block, the decryption unit would receive the key stream in the same order. Therefore, when the decryption unit stores the key stream to perform the decryption operation, the keys would be mapped in the memory to a respective encrypted data block. Warren does not disclose having different size data blocks identified by an offset value. Rump discloses a system for encryption and decryption of multi-media data wherein each block contains a block size index (Col. 7, line 18), which meets the limitation of the size of said single data block is further conditioned by an offset value, the size of each successive data block is based on an average size and based on randomly generated offset. The block size indexes can be different corresponding to different sizes (Col. 7, lines 18-35), which would also meet the limitation of each block comprising plural image frames, some of the blocks are of different sizes in terms of number of frames from other blocks. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the variable block sizes in the multi-media copy management system of Warren in order to simplify and streamline multi-media data processing as taught in Rump (Col. 7, lines 18-35).

Referring to claim 2,Warren discloses that the receiver contains a decryption engine (Fig. 17) to decrypt the encrypted multi-media stream with the encryption keys that are embedded in the stream (Fig. 12, Col. 13, line 58 – Col. 14, line 3), which meets the limitation of digital receiver includes a decryption engine which is responsive to said encryption key and said encryption engine and decryption engine are provided with symmetric encryption, the encrypted data blocks comprise digital motion image data blocks and the digital motion image data blocks are decrypted by providing a digital motion image data frame or digital motion image data frame component identification; and generating a corresponding key from the plurality of encryption keys for use in decrypting the block of which the frame or frame component forms a part.

Referring to claim 5, Warren discloses that the communication channel can be a satellite channel (Col. 1, lines 22-24), which meets the limitation of the data transmission channel being a wireless transmission network.

Referring to claim 6, Warren discloses that the communication channel can be a telephone network (Col. 6, line 40), which meets the limitation of a data transmission channel that utilizes dedicated phone service.

Referring to claims 7, 13, 16, Warren discloses that the communication network uses a portable storage medium (Col. 1, lines 10-15).

Referring to claims 8-10, Warren discloses that the communication network can be cable networks, The Internet, or intranets (Col. 1, lines 22-23), which meets the limitation of a computer data network, wide area network and a local area network.

Referring to claim 15, Warren discloses that the channel that the encryption keys are distributed on can be encrypted (Col. 16, lines 16-24 & Fig. 12).

Referring to claim 17, Warren discloses that the data can be compressed (Col. 2, lines 31-33), which meets the limitation of single data block is compressed.

Referring to claim 52, Warren disclo3ses that the receiver contains a decryption engine (Fig. 17) to decrypt the encrypted multi-media stream with the encryption keys that are embedded in the stream (Fig. 12, Col. 13, line 58 – Col. 14, line 3), which meets the limitation of digital receiver includes a decryption engine which is responsive to said encryption key and said encryption engine and decryption engine are provided with symmetric encryption, the encrypted data blocks comprise digital motion image data blocks and the digital motion image data blocks are decrypted by providing a digital motion image data frame or digital motion image data frame component identification; and generating a corresponding key from the plurality of encryption keys for use in decrypting the block of which the frame or frame component forms a part. Warren discloses that the compression can be done using MPEG compression methods (Col. 5, line 4).

Referring to claim 21, Warren discloses that the encrypted data is recorded on a medium (Fig. 15, 140).

Referring to claim 22, Warren discloses that the medium is floppy disks or magnetic tapes (Col. 1, lines 27-28), which meets the limitation of magnetic storage technology.

Referring to claim 23, Warren discloses that the medium is a CD of DVD (Col. 1, lines 13-15), which meets the limitation of an optical medium.

Referring to claim 24, Warren discloses the multi-media data stream is transmitted over a data channel (Col. 2, lines 27-34), which meets the limitation of providing said encrypted data block comprises the step of transmitting said encrypted data block to the digital data receiver.

Referring to claim 25, Warren discloses that the channel that the encryption keys are distributed on can be encrypted (Col. 16, lines 16-24 & Fig. 12).

Referring to claim 27, Warren discloses that the multi-media data is video (Abstract), which meets the limitation of digital motion image data.

Referring to claim 51, Warren discloses that the data can be compressed (Col. 2, lines 31-33), which meets the limitation of single data block is compressed.

10. Claims 11, 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Handelman, U.S. Patent No. 5,774,546. Referring to claims 11, 14, Warren discloses a copy management system for multi-media wherein multi-

media data is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56), which meets the limitation of an encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks. Figure 12 shows explicitly that each data block contains the encryption key for the frame contained in the next data block, which meets the limitation of block synchronization index indicating a correspondence between said encryption key and single data block. Figure 12 shows a multi-media data stream that has been encrypted with the corresponding keys (Col. 13, line 58 – Col. 14, line 3), which meets the limitation of an encryption engine that, for each said single data block, produces an encrypted data block using said encryption key fro said encryption key generator. The multi-media data stream is transmitted over a data channel (Col. 2, lines 27-34), which meets the limitation of a data transmission channel for delivering said encryption data block from said encryption engine to the digital data receiver. The multi-media data stream could include a plurality of data channels, with one of the data channels including the encryption key data (Col. 2, lines 27-34), which meets the limitation of a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver. As specified above, the encryption key data also provides the means for the block synchronization as disclosed in Figure 12, which meets the limitation of a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver. Warren does not disclose using smart cards in the copy management system. Handelman discloses a data access system wherein video data is accessed using a smart card that communicates seeds, keys, and access control algorithms with the video decoder (Col. 2, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use smart cards in the copy management system of Warren in order to provide secure access to restricted means as taught in Handelman (Col. 1, line 18).

11. Claims 12, 18, 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909. Referring to claim 18, Warren discloses that the system can use a number of different associations between the encryption keys and the data frames (Col. 3, lines 18-27), but Warren does not disclose that this association is chosen randomly. It would have been obvious to one of ordinary skill in the art at the time the invention was made to randomly choose the association between the encryption keys and the data frames in order to make the copy protection harder to break.

Referring to claims 12, 31, Warren does not disclose that this association is encrypted, but it would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt this association between the encryption keys and the data frames in order to shield this security association, that is necessary for copy protection, from would be pirates.

12. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Schneier. Referring to claim 19, Warren does not disclose that linear feedback shift registers can randomly generate the associations. Schneier discloses that pseudo-random sequences can be generated using linear feedback shift registers (Page 373). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the pseudo-random sequences of Warren to be generated using a linear feedback shift register because shift registers have been used to generate stream ciphers since the beginning of electronics as taught in Schneier (Page 372).

13. Claims 26, 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Dahan, U.S. Patent No. 6,137,763. Referring to claims 26, 37, Warren discloses that data is stored on optical mediums (Col. 1, lines 13-15) and transferred sequentially (Fig. 13) as opposed to non-sequentially. Dahan discloses a method of buffering data read from an optical disk wherein the data is read from the disk in a non-sequential order (Col. 2, lines 32-42). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the data of Warren to be transmitted in non-sequential order because Dahan discloses that non-sequential reads of optical disks occur, and would therefore need a correctional mechanism to insure that correct sequencing occurs. It would be obvious to eliminate this correction step to lower production costs and processing time.

14. Claims 42, 45, 46, 50, 53-56, 76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Chaum, U.S. Patent No. 5,959,717. Referring to claims 42, 50, Warren does not disclose that the video signal can be decoded at a projector. Chaum discloses a copy protection system that utilizes two video parts in combination at the projector to view the film (Col. 1, line 46 – Col. 2, line 54). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the decoder of Warren to be housed in a projector because film projection systems are the dominate way to publicly screen motion pictures as taught in Chaum (Col. 1, lines 12-14).

Referring to claims 45, 46, 53-56, 76, Warren does not disclose that the video signal is encrypted based on color data. Chaum discloses that rather than performing frame by frame protection of the film, protection can be performed on a color basis (Col. 5, lines 14-17). It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the video data of Warren with respect to color in order to produce holes in the video content so that theft or piracy would be less desirable as taught in Chaum (Col. 5, lines 16-30).

Claims 70, 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Rabowsky, U.S. Patent No. 6,141,530. Referring to claims 70, 71, Warren discloses a copy management system for multi-media wherein multi-media data is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56), which meets the limitation of an encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks. Figure 12 shows explicitly that each data block contains the encryption key for the frame contained in the next data block, which meets the limitation of block synchronization index indicating a correspondence between said encryption key and single data block. Figure 12 shows a multi-media data stream that has been encrypted with the corresponding keys (Col. 13, line 58 – Col. 14, line 3), which meets the limitation of an encryption engine that, for each said single data block, produces an encrypted data block using said encryption key fro said encryption key generator. The multi-media data stream is transmitted over a data channel (Col. 2, lines 27-34), which meets the limitation of a data transmission channel for delivering said encryption data block from said encryption engine to the digital data receiver. The multi-media data stream could include a plurality of data channels, with one of the data channels including the encryption key data (Col. 2, lines 27-34), which meets the limitation of a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver. As specified above, the encryption key data also provides the means for the block synchronization as disclosed in Figure 12, which meets the limitation of a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver. Warren does not disclose that the data stream contains a motion picture name or a theater name. Rabowsky discloses a digital electronic cinema system wherein motion picture files are transmitted with the file name and a specific theater name (Col. 1, line 47 – Col. 2, line 47). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a file name and theater name with the data stream in Warren in order to transmit a specific film to a specific theater electronically as taught in Rabowsky (Col. 1, lines 39-44).

(10) Response to Argument

Applicant's argument with respect to the antecedent basis issue with claim 3 is not persuasive because Applicant's cancelled out all recitations of "single data block" in the independent claim 1, but forgot to correct claim 3 according to the amendments, which left the antecedent basis issue.

Applicant's argument, paragraph number 2 on page 7, with respect to the 112 first issue is persuasive and the rejection is withdrawn.

Applicant's argument that claims 62-71 are statutory is not persuasive because they disclose a data structure that is not embodied within a computer readable medium. A data structure by itself is non-statutory subject matter, but if the data structure was embodied within a computer readable medium, it would be considered statutory. MPEP 2106.

Applicant's argument that Warren does not disclose a synchronization index is not persuasive because Warren discloses (Figures 12 & 13) that the key stream layer (1250) of the data stream provides synchronization in that the stream contains the cryptographic keys for the data blocks with an identifier for which block it belongs. Therefore, for the purposes of decryption this key stream layer would act as a synchronization index because it would synchronize a key block with a corresponding data block for decryption purposes. A clear indication of this is given in figures 12 and 13, when viewing the key stream layer (1250). Each key block corresponds to a specific data block. Key block 1223 contains the key for data block 2 (1240), and key block 1243 contains the key for data block 3 (1260), and so on.

Applicant's argument that this synchronization index being generated is not persuasive because Warren discloses that the encryption key blocks of the key stream layer can be compiled in any order because of the buffering capabilities of the processing units (Col. 14, line 61 – Col. 15, line 8). Therefore, the key stream layer is generated because the key stream layer can be generated for a specific association with the data frames (Col. 14, lines 4-18).

Applicant's argument with respect to claim 36, that Warren doesn't disclose mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks of a digital motion image is also not persuasive for the same reasons given above. While the key stream layer would be considered to be acting as a synchronization index for the decryption process, the key stream layer is also mapping a specific key to a specific data block for the decryption process (Figures 12 & 13). Key block 1223 contains the key for data block 2 (1240), and key block 1243 contains the key for data block 3 (1260), and so on. This is a clear example of mapping a key to a specific data block of a digital motion image.

Applicant's argument that Warren does not disclose padding the plurality of encryption keys using dummy bits because Warren discloses that some keys may be null keys so that these null keys can be used with unencrypted frames and that the null keys are not associated with encrypted frames and this do not comprise encryption keys that correspond to a plurality of encrypted data blocks is not persuasive because the claims (i.e. 38) only requires "the step of padding said plurality of encryption keys using dummy bits". Warren meets this claim limitation because the entire key stream layer represents the claimed plurality of encryption keys, and the teaching of having null keys (all zeros or "dummy bits") would meet the limitation of padding the plurality of encryption keys because the null keys would have to fit a certain field within the key stream and would be considered padding. The claims do not require the padded keys to be associated with an encrypted frame.

Applicant's argument that Warren does not disclose generating a key corresponding to a pertinent data block using a frame or frame component identification is not persuasive as mentioned above, Warren discloses (Figure 12 & 13) a key stream layer that contains keys that directly correspond to a specific data block that contains a frame identifier. Therefore, when the keys where generated they were generated specifically for the frame, identified by the frame identifier, that exists in the corresponding data block.

Applicant's argument that the Examiner has given no specific comments with regard to the anticipated of claim 52 is not persuasive because claim 52 is fully address on pages 14-15 of the office action dated 29 August 2005.

Applicant's argument with respect to claim 52, that Warren does not disclose encrypted the P and B frames of the MPEG data stream is not persuasive because Warren discloses the use of MPEG compression (Col. 5, line 4) and the entire signal is encrypted in Warren (Col. 14, lines 24-27) therefore the intra coded and P and B frames are encrypted as claimed.

Applicant's arguments with respect to claim 63 are not persuasive because figures 12 & 13 show the start of the data structure.

Applicant's argument that Warren does not disclose "information specifying an algorithm used to locate a corresponding key within the key field" is not persuasive because Warren discloses that one scenario for the system could have each key block N of the key stream, would have the key for data block N+1 (Col. 14, lines 12-17). N+1 is an algorithm used to locate a corresponding key within the key field.

Applicant's arguments with respect to claims 12, 18, and 31, rely on the belief that Warren does disclose a "synchronization index", which has been fully addressed above.

Applicant's argument that the prior art does not disclose that each data block comprises plural frames is not persuasive because Rump discloses that the data blocks comprise a plurality of frames (Col. 7, lines 18-35). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the variable block sizes in the multi-media copy management system of Warren in order to simplify and streamline multi-media data processing as taught in Rump (Col. 7, lines 18-35).

In response to applicant's arguments against the references individually (Warren and Rump), one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Applicant's argument the Warren does not disclose encryption of the encryption keys is not persuasive because the encryption keys of Warren are in the key stream layer of the data stream, and the entire data stream of Warren is encrypted (Col. 14, lines 24-27). Therefore, the encryption keys of Warren are encrypted.

Applicant's argument that the combination of Warren and Rump is based on a conclusory statement is not persuasive because a motivation as to why one of ordinary skill in the art at the time the invention was given was provided directly from the prior art references.

Applicant's argument that the Warren reference does not disclose information relative to the encryption keys being provided over a different channel than the channel that is providing the cipher text is not persuasive because figures 12 and 13 of Warren show separate channels for the encryption keys and the encrypted information (cipher text).

Applicant's argument that the Warren reference does not disclose the synchronization field and the keys in the key field creating a table or matrix in the memory that maps each key to its respective image block is not persuasive because memory is already formatted in a table structure. Each cell of memory having an address and space for data, and when the decryptor uses key stream layer to decrypt the encrypted data blocks the data from these layers would be placed in memory so that they could be processed. The key stream information that was discussed above would still be present, and therefore, the mapping of keys to blocks is present. The actual presence of a memory unit is discussed in Warren (Col. 9, line 66 – Col. 10, line 5).

In response to applicant's arguments against the references individually (Warren and Handelman), one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Applicant's argument that the combination of Warren and Schneier is based on a conclusory statement is not persuasive because a motivation as to why one of ordinary skill in the art at the time the invention was given was provided directly from the prior art references.

In response to applicant's arguments against the references individually (Warren and Chaum), one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Applicant's argument that no motivation was given for the combination of Warren and Chaum to meet the limitations of claim 46 is not persuasive because motivation for the combination can be found in the final office action dated 29 August 2005, on pages 18-19.

Applicant's arguments with respect to claim 50 (page 29 of the Appeal Brief) are not persuasive because Applicant is arguing limitations that are not found in claim 50. Claim 50 requires "the decryption of the encrypted data blocks is made in a digital motion image projector which projects images represented by the digital motion image data upon a screen". This limitation has been fully addressed in the final office action date 29 August 2005 on page 18.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Applicant's argument that the cited disclosure of Rabowsky cannot meet the limitation of a key overhead field that contains a movie name and theater name is not persuasive because the location with the film data that contains the film and theaters names in Rabowsky would be structurally equivalent. The fact that Rabowsky does not say, "key overhead field" is irrelevant.

Applicant's arguments that claims 29 and 51 have not been address in the rejections is not persuasive because claim 51 was fully addressed in the final office action dated 29 August 2005 on page 15. Claim 29 was fully addressed in the office action dated 15 April 2005 on pages 7-8, but was inadvertently omitted from the final office action. No new grounds of rejection have been made, because the rejection of claim 29 in the above mentioned office action is still applicable.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Benjamin E. Lanier

Conferees:

Gilberto Barron

Justin Darrow

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100